SonicWALL Mobile Connect

Mobile Connect for Android 3.0 User Guide

SONICWALL®

Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your system.

CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

© 2014 SonicWALL LLC.

Trademarks: SonicWALL™, Aventail™, SonicWALL Mobile Connect™, and all other SonicWALL product and service names and slogans are trademarks of SonicWALL LLC., a wholly owned subsidiary of Dell.

2014 – 4 P/N 232-002407-00 Rev. A

Table of Contents

How Mobile Connect Works 5
Prerequisites 5
- Android Product Support 6
- Dell SonicWALL Appliance Support 6
- What's New in This Release? 6
- Required Network Information 7

Installing Mobile Connect 8
Using Mobile Connect 8
- Creating a Connection 9
- Connecting to the Mobile Connect Server 12
- Configuring Mobile Connect Settings 16
- URL Control Syntax and Parameters 18
- Callback URL 21
- Bookmarks 23
- Files 25

Configure Client Certificates 30
- Configuring a Connection to Dell SonicWALL E-Class SRA Appliances 30
- Configuring a Connection to Dell SonicWALL SMB SRA Appliances 32

Monitoring Mobile Connect 34
Mobile Connect Widget 36
Troubleshooting Mobile Connect 37

Using Mobile Connect for Android

SonicWALL Mobile Connect for Android™ is an **app** that enables Android devices to establish secure, mobile connections to private networks protected by Dell SonicWALL security appliances.

How Mobile Connect Works

Modern business practices increasingly require that users be able to access any network resource (files, internal websites, etc.), anytime, anywhere. At the same time, ensuring the security of these resources is a constant struggle. While most users are aware that they must take care to protect computers from network security risks, this security awareness does not always extend to mobile devices. And yet, mobile devices are increasingly subject to security attacks. Furthermore, mobile devices often use insecure, untrusted, public Wi-Fi hotspots to connect to the Internet. It is therefore a challenge to provide secure, mobile access while still guarding against the inherent security risks of using mobile devices.

The SonicWALL Mobile Connect app for Android devices provides secure, mobile access to sensitive network resources. Mobile Connect establishes a Secure Socket Layer Virtual Private Network (SSL VPN) connection to private networks that are protected by Dell SonicWALL security appliances. All traffic to and from the private network is securely transmitted over the SSL VPN tunnel.

To get started with SonicWALL Mobile Connect:

1. Install SonicWALL Mobile Connect from the Google Play Store or the Amazon Appstore.
2. Enter connection information (server name, username, password, etc.).
3. Initiate a connection to the network.
4. Mobile Connect establishes a SSL VPN tunnel to the Dell SonicWALL security appliance.
5. You can now access resources on the private network. All traffic to and from the private network is securely transmitted over the SSL VPN tunnel.

Prerequisites

The following sections describe prerequisites for SonicWALL Mobile Connect:

- Android Product Support on page 6
- Dell SonicWALL Appliance Support on page 6
- Required Network Information on page 7

Android Product Support

SonicWALL Mobile Connect requires the Android 4.0 or newer platform and a cellular or Wi-Fi connection.

SonicWALL Mobile Connect has been verified to run on the following Android devices running the official Android 4.0 platform:

- Dell Venue 7 and 8
- Samsung Nexus 10
- Samsung Galaxy S2
- Samsung Galaxy S3
- Samsung Galaxy Tab
- ASUS Nexus 7
- ASUS FonePad
- LG Nexus 4
- Motorola Droid Razr Tablet
- Amazon Kindle Fire

Note Although Mobile Connect is designed to work with all Android devices running the 4.0 or newer platform, only the above platforms have been tested and verified to run Mobile Connect. Custom ROMs are not officially supported.

Dell SonicWALL Appliance Support

SonicWALL Mobile Connect is a free app, but requires a concurrent user license on one of the following Dell SonicWALL solutions in order to function properly:

- Dell SonicWALL firewall appliances including the TZ, NSA, E-Class NSA running SonicOS 5.8.1.0 or higher
- Dell SonicWALL SRA appliances running 5.5 or higher
- Dell SonicWALL Aventail E-Class SRA appliances running 10.5.4 or higher

What's New in This Release?

The following features, some of which are specific to E-Class SRA appliances or SMB SRA appliances and Next Generation Firewalls, have been added in Mobile Connect 3.0:

- **UI Redesign** – Mobile Connect 3.0 has a new app icon, splash screen, and look and feel. The **Connect**/**Disconnect** button has been replaced with an **On**/**Off** switch.
- **File Bookmarks** – Mobile Connect 3.0 working with SRA 7.5 firmware introduces secure mobile access to files. Granular policy controls can be configured to allow other Android apps to use each file. Policies include control over whether a file may be securely cached or opened in a third party app. Files Bookmarks are displayed after the VPN is connected. Selecting a Files bookmark checks and enforces the server policy, securely downloads the file, and displays it within the appropriate app. Bookmarks to folders or file share root directories can also be created to allow for directory navigation.

  At this time File bookmarks are supported only in SMB SRA appliances running SRA 7.5 firmware. File bookmark support in the E-Class SRA and Next Generation Firewalls is expected in a future release.

E-Class SRA Features

- **Credential Caching** – Users may now cache their username and password credentials to reduce the burden of managing their credential identities to gain access. This feature requires 10.7.x E-Class SRA firmware.

- **Network Awareness** – VPN connections can be configured to detect whether the user is remote or on premise and control the VPN connection accordingly. This feature requires 10.7.x E-Class SRA firmware.
- **IPv6 Phase I Support** – VPN connections can connect to SRA EX appliances via IPv6 and access IPv6 resources over the VPN. This feature requires 10.7.x E-Class SRA firmware.
- **TLSv1.1/1.2 Support** – This feature requires 10.6.4+ or 10.7.x E-Class SRA firmware.

SMB SRA & Next Generation Firewall Features

- **Client Certificate Authentication Support** – Client certificate authentication is now available for SRA appliance connections. If a client certificate is required during authentication, the user will be automatically prompted to select a client certificate from the Android device client certificate store.
- **Compression** – Traffic over the VPN tunnel is compressed using the LZ4 algorithm when connected to a server that supports compression and has it enabled for the tunnel. A Compression row displaying the overall compression ratio is shown on the Monitor tab if compression is enabled. This feature requires 7.5 SRA firmware.
- **End Point Control** – End Point Control policy checking is performed before establishing the VPN connection established. Mobile Connect supports the following attributes:
  - Application
  - Directory name
  - File name
  - Equipment ID
  - Android version

  This feature requires 7.5 SRA firmware.

Required Network Information

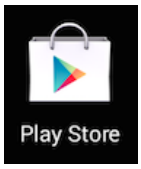
In order to use SonicWALL Mobile Connect, you will need the following information from your network administrator or IT support:

- Server name or address – This is either the IP address or URL of the SSL VPN server that you will connect to.
- Username and password – Typically, you will be required to enter your username and password, although some connections may not require this.
- Domain name – The domain name of the SSL VPN server. Mobile Connect may be able to automatically determine this when it first contacts the server, or there may be multiple domains that can be selected.

Installing Mobile Connect

SonicWALL Mobile Connect is installed through the Google Play Store or the Amazon Appstore.

1. On your Android device, tap the Google Play icon:

   Or, type the following in the browser:

   Google Play Store:
   https://play.google.com/store/apps/details?id=com.sonicwall.mobileconnect

   Amazon Appstore:
   https://www.amazon.com/gp/mas/dl/android?p=com.sonicwall.mobileconnect
2. Go to the **Search** tab, type **SonicWALL Mobile Connect**, and tap **Search**.
3. In the search results, select **SonicWALL Mobile Connect**.
4. Click the **Install** button under **SonicWALL Mobile Connect**. The app will install on your device. When installation is complete, the SonicWALL Mobile Connect icon will appear on your device.

If you encounter an error when attempting to download SonicWALL Mobile Connect, please go to the appropriate site for help:

Google Play Store Help - Follow troubleshooting procedures and instructions on how to report the issue using your Google account: http://support.google.com/googleplay/?hl=en

Amazon Appstore Help - Follow troubleshooting procedures and instructions on how to report the issue using your Google account:
http://www.amazon.com/gp/help/customer/display.html?nodeid=201111910

Using Mobile Connect

The following sections describe how to use Mobile Connect:

- Creating a Connection on page 9
- Connecting to the Mobile Connect Server on page 12
- Configuring Mobile Connect Settings on page 16

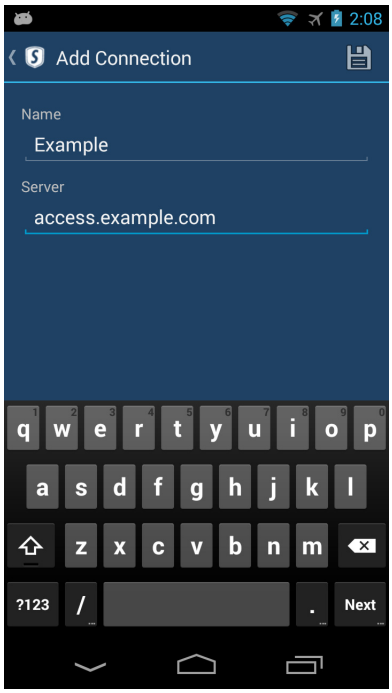
Creating a Connection

The process of creating a Mobile Connect connection is slightly different depending on which type of Dell SonicWALL appliance you are connecting to. The following sections describe how to create a connection:

- Creating a Connection to Dell SonicWALL Firewall and SRA Appliances on page 9
- Creating a Connection to Dell SonicWALL E-Class SRA Appliances on page 11

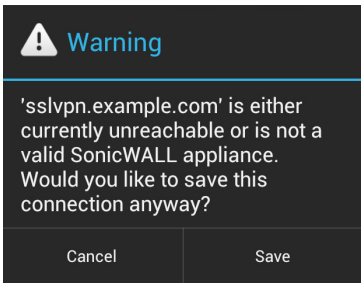
Creating a Connection to Dell SonicWALL Firewall and SRA Appliances

1. Launch SonicWALL Mobile Connect. You will be presented with the screen to begin your first connection. Tap **Add connection**.
   - **Name**: Enter a descriptive name for the connection.
   - **Server**: Enter the URL or IP address of the server.



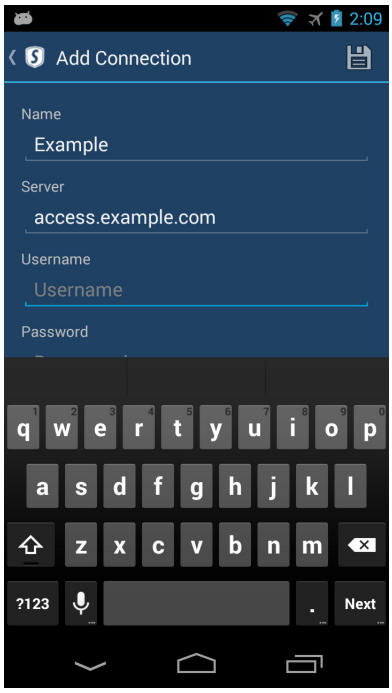
2. Tap **Next**. Mobile Connect will then attempt to contact the Dell SonicWALL appliance.

   If the attempt fails, a warning message will display, asking if you want to save the connection. Verify that the server address or URL is spelled correctly, and then tap **Save**.


Warning
'sslvpn.example.com' is either currently unreachable or is not a valid SonicWALL appliance. Would you like to save this connection anyway?
Cancel
Save

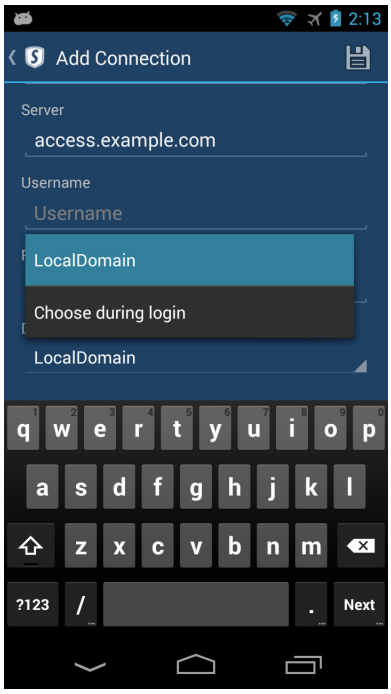
3. Before tapping **Save**, verify that the server address or URL is spelled correctly.

4. If Mobile Connect successfully contacts the server, you will be prompted to enter your **Username** and **Password** (unless the server does not require this information).



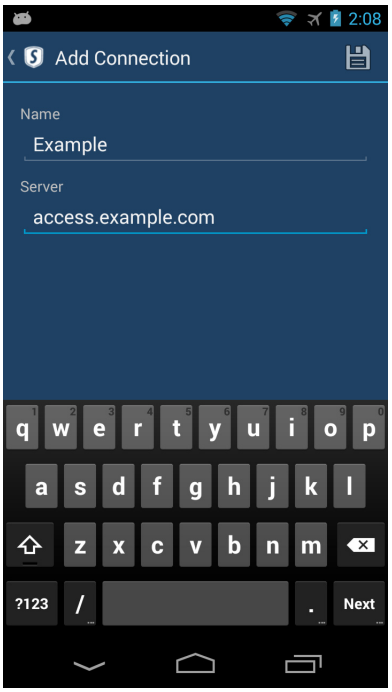
Note If the screenshots above do not match what is displayed on your device, you are connecting to a Dell SonicWALL E-Class SRA appliance. Proceed to Creating a Connection to Dell SonicWALL E-Class SRA Appliances on page 11.

5. The **Domain** field is auto-populated with the default domain from the server. To select a different domain, tap **Domain** to display a drop-down menu of the available options and tap **Save**.

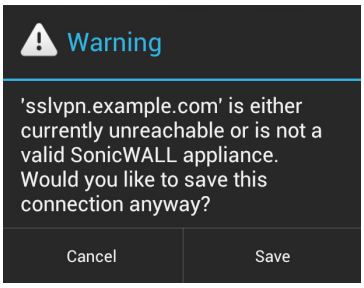


Creating a Connection to Dell SonicWALL E-Class SRA Appliances

1. Launch Mobile Connect. You will be presented with the screen to begin your first connection. Tap **Add connection**.
   - **Name**: Enter a descriptive name for the connection.
   - **Server**: Enter the URL or IP address of the server.



2. Tap **Next**. Mobile Connect will then attempt to contact the Dell SonicWALL appliance. If the attempt fails, a warning message will display, asking if you want to save the connection.

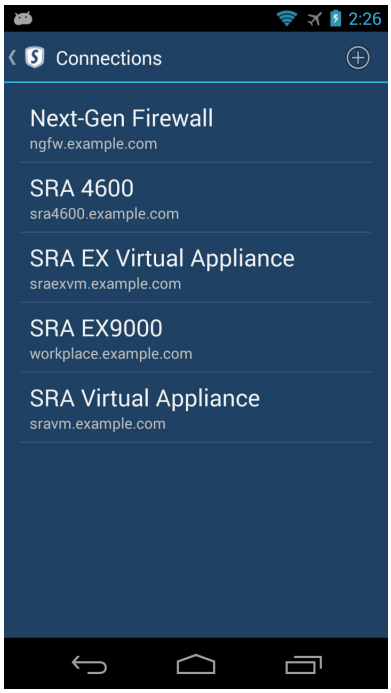

Warning
'sslvpn.example.com' is either currently unreachable or is not a valid SonicWALL appliance. Would you like to save this connection anyway?
Cancel
Save

3. Before tapping **Save**, verify that the server address or URL is spelled correctly.

   If Mobile Connect successfully contacts the server, the connection will be automatically saved.

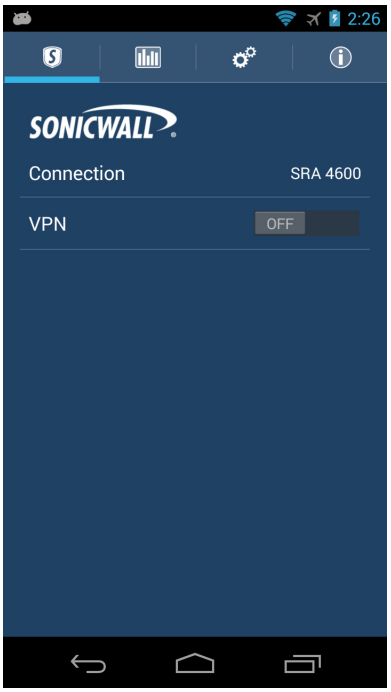
Connecting to the Mobile Connect Server

After you save a new connection, the list of all configured connections displays.

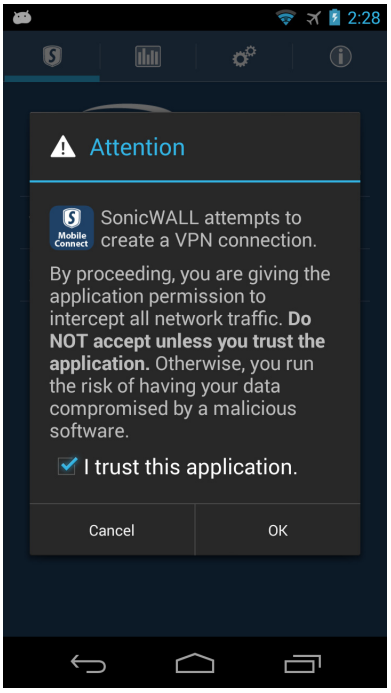


To establish a Mobile Connect session, perform the following tasks:

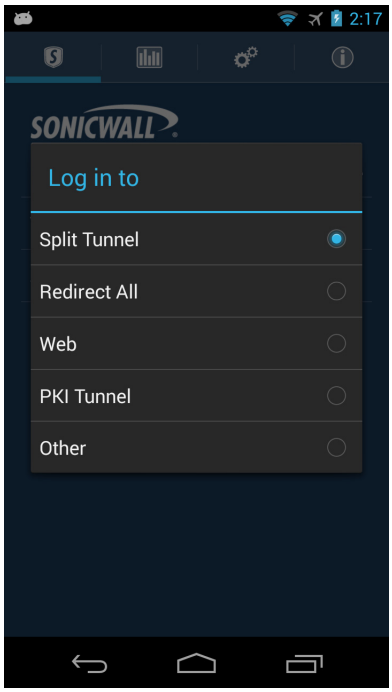
1. Tap the connection in the list that you want to initiate. The **Connection Status** page displays. Tap **VPN** ON/OFF switch.



2. The first time you initiate a connection, a warning message displays. Tap the **I trust this application** checkbox, and then tap **OK**.

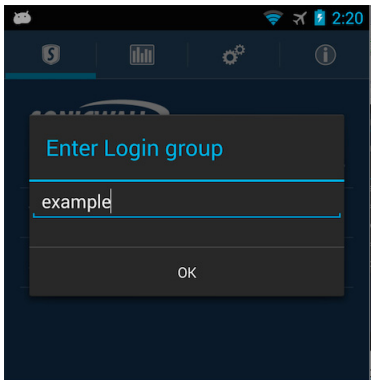

2:28
Attention
SonicWALL attempts to create a VPN connection.
By proceeding, you are giving the application permission to intercept all network traffic. Do NOT accept unless you trust the application. Otherwise, you run the risk of having your data compromised by a malicious software.
I trust this application.
Cancel
OK

3. **For E-Class SRA connections only:** If Mobile Connect successfully contacts the server, you will be prompted to select which Login Group on the appliance you want to connect to. If you do not know which Login Group to connect to, contact your network administrator.

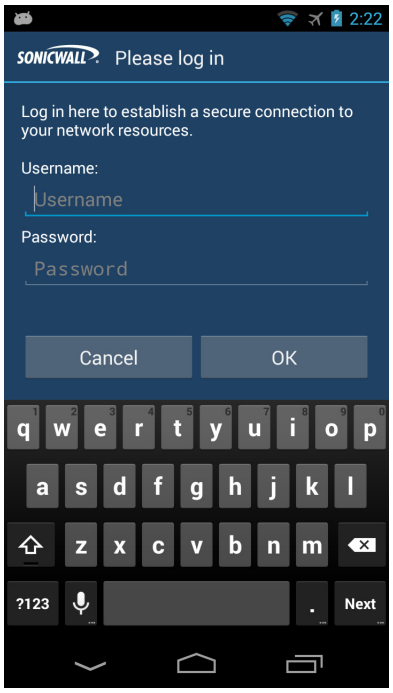


Note If the screenshots above do not match what is displayed on your device, you are connecting to a Dell SonicWALL firewall or SRA appliance. Proceed to Creating a Connection to Dell SonicWALL Firewall and SRA Appliances on page 9, step 4.

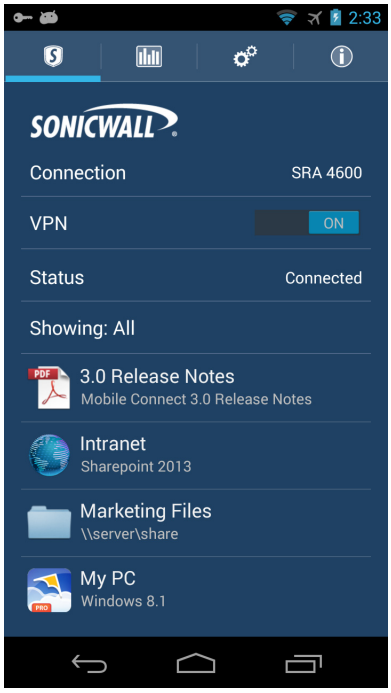
4. **For E-Class SRA connections only:** If the Login Group you connect to is not listed, select **Other...** to manually type in the group name.



5. **For E-Class SRA connections only:** Enter your username and password if prompted (depending on whether the Dell SonicWALL appliance you are connecting to allows for saving usernames and passwords).

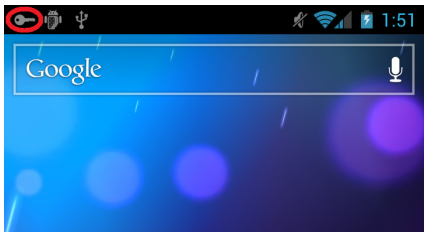


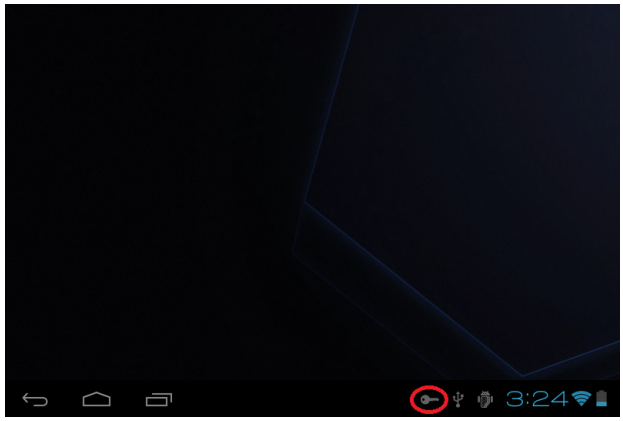
When the connection is successfully established, the **Status** changes to **Connected** and the VPN switch remains in the ON position.



Any bookmarks defined for the portal are displayed below the Disconnect button. Navigate to a bookmark's destination.Bookmarks will only appear after a VPN connection is established if the server is running firmware that supports Mobile Connect bookmarks and bookmarks have been defined for that user.

6. Press the **Home** button to return to your device's home screen. You can now navigate to other apps to access your Intranet network. The status bar will display a VPN icon to indicate that the session is still connected.



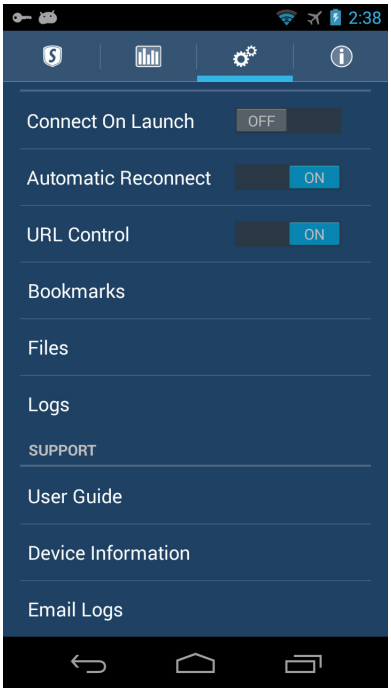


If the VPN connection is interrupted, the VPN icon will disappear and you will no longer be able to access the Intranet network. This can happen if your device's connection transitions to a different network connection (for example, from Wi-Fi to cellular).

Return to Mobile Connect to reestablish the connection. Optionally, you can configure the **Automatic Reconnect** option on the **Settings** tab to have Mobile Connect automatically attempt to reestablish interrupted connections.

Configuring Mobile Connect Settings

SonicWALL Mobile Connect provides several settings for connection and logging options. The Settings tab also provides Support information, which includes a User Guide and device, connection, and server information.



The following options are controlled from the Settings tab:

- **Connect on Launch** - Sets Mobile Connect to automatically initiate a connection to the last-used profile when it is launched.
- **Automatic Reconnect** - Sets Mobile Connect to automatically attempt to reconnect if the connection is lost. The SSL VPN connection can be disrupted when your device's connection transitions to a different network type (for example, from Wi-Fi to 3G). This setting lets applications rely on a sustained VPN connection. There is no limit on the amount of time it takes to reconnect.
- **URL Control** - Allows other mobile applications to pass action requests using special URLs to Mobile Connect. These action requests can create VPN connection entries and connect or disconnect VPN connections. For example, another application can launch Mobile Connect, access internal resources as needed, and then disconnect by using the mobileconnect:// or sonicwallmobileconnect:// URL scheme. Some common examples of URL Control are:

  Add profile: **mobileconnect://addprofile**[/]**?name=***ConnectionName***&server=***ServerAddress*[**&***Parameter1***=***Value***&***Parameter2***=***Value...*]

  Connect: **mobileconnect://connect**[/]**?[name=***ConnectionName*|**server=***ServerAddress*][**&***Parameter1***=***Value***&***Parameter2***=***Value...*]

  Disconnect: **mobileconnect://disconnect[/]**

  Additional information about URL Control is provided in URL Control Syntax and Parameters on page 18.

- **Bookmarks** - Displays centrally configured shortcuts (called bookmarks) to VPN resources like web pages, Remote Desktop servers, and terminal servers. These bookmarks, which are displayed on the main Connection tab when the VPN is connected, provide one-touch access to frequently used applications.

  If using a SRA appliance, pulling down the Connection screen and releasing it refreshes the bookmarks. Mobile Connect supports Remote Desktop options like screen size and enable/disable audio as long as both the server bookmark and third party application support the option.

  Note Bookmarks are supported on SRA appliances only when running 7.0 or higher and not supported on UTM appliances running SonicOS.

  Additional information about bookmarks is provided in Bookmarks.

- **Files > Delete Cached Files** - Deletes all cached files that have been downloaded and stored on the device. Note that cached files are stored encrypted on the device for added security.

  Note Files are supported on SRA appliances only when running 7.5 or higher and not supported on appliances running SonicOS.

  Additional information about Files is provided in Files.

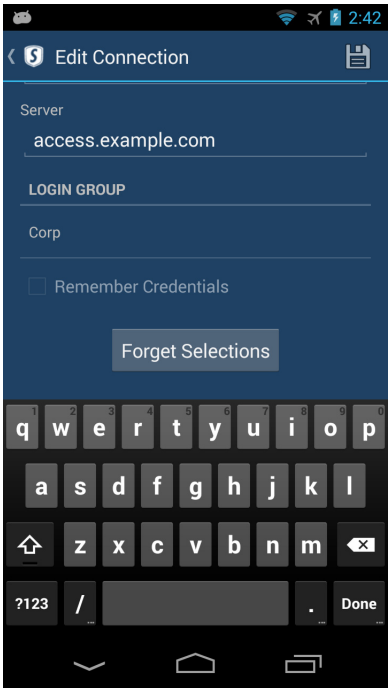
- **Logs > Debug Logging** - Enables full debug log messages of Mobile Connect activity. Leave this setting disabled unless instructed to enable it by Dell SonicWALL Support staff.
- **Logs > Clear Logs** - Deletes all log files saved on the device.

The **Support** section of the Settings tab provides the following support information:

- **User Guide** - Displays the SonicWALL Mobile Connect User Guide.
- **Device Information** - Displays information about the device, Wi-Fi connection, Cellular connection, and DNS servers.
- **Email Logs** - Creates an email to send the Mobile Connect log to Dell SonicWALL Support staff. Tap **Send** to send the email.

E-Class SRA Settings

Connections to Dell SonicWALL E-Class SRA appliances have two additional options that are available on the **Edit Connection** window. To view this option, go to the **Connection** tab and tap and hold on the Connection line to bring up the **Edit Connection** window.



The following options can be configured:

- **Remember Credentials** - Enables saving of user authentication credentials for the VPN connection. This is enabled by default and can be controlled by the E-Series SRA server setting.
- **Forget Selections** - Mobile Connect remembers the Login Group that you specified when configuring the connections. To change to a different Login Group, tap **Forget Selections**. The next time you connect to the server, you will be prompted to select a new Login Group.

Note If this option is not displayed, you are connecting to either a Dell SonicWALL firewall or SRA appliance.

URL Control Syntax and Parameters

This section provides the full set of URL parameters for the URL Control feature. URL Control currently supports the addprofile, connect, and disconnect commands. Callback URLs are also supported.

Add Profile Command

The addprofile command requires either the name or server parameter, and accommodates both. All other parameters are optional. When the URL is opened in Mobile Connect, all of the parameters included in the URL are saved in the connection entry associated with that name and server.

Syntax:

mobileconnect://addprofile[/]?name=*ConnectionName***&server=***ServerAddress*
[**&***Parameter1***=***Value***&***Parameter2***=***Value...*]

Following are examples of the addprofile command:

```
mobileconnect://addprofile/?name=Example&server=vpn.example.com
sonicwallmobileconnect://addprofile/?name=Example&server=vpn.example.com
mobileconnect://addprofile?name=Example%202&server=vpn.example.com
mobileconnect://addprofile?name=vpn.example.com
mobileconnect://addprofile?server=vpn2.example.com
mobileconnect://addprofile?name=SRA%20Connection&server=sslvpn.example.com&
username=test&password=password&domain=LocalDomain&connect=1
mobileconnect://addprofile?name=EX%20Connection&server=workplace.example.com&
username=test&password=password&realm=Corp&connect=1
```

Note All appropriate characters in values of parameters used in URLs are required to be URL encoded. For instance, to match a space, enter %20.

Add Profile Command Parameters

Command Parameter	Description
name	The unique name of the VPN connection entry that will be created and appear in the Mobile Connect Connections list. Mobile Connect accepts the name only if it is unique. Letters are case sensitive.
server	The domain name or IP address of the Dell SonicWall appliance in which you wish to connect. For example: vpn.example.com
username	**Optional**: The username used in the VPN connection.
password	**Optional**: The password used in the VPN connection.
realm	**Optional**: The realm used in the VPN connection profile. Applies to EX series connections only.
domain	**Optional**: The domain used in the VPN connection profile. Applies to SRA and UTM connections only.
sessionid	**Optional**: The session ID or Team ID used for authentication.
connect	**Optional**: If presented and the value is non-null, the connection will be initiated if the profile was successfully added.
callbackurl	**Optional**: The callback URL is be opened by Mobile Connect after the add profile command has been processed. See Add Profile Command on page 18 for full details of the callback URL syntax and options.

Connect Command

The connect command is used to easily establish VPN connections. Connection information can be embedded in the URLs and they can be provided to users for easy setup and configuration. In addition, a callback URL can be provided that Mobile Connect will open after the connection attempt is completed, making it possible for other applications to initiate VPN connections in a seamless manner.

Syntax:

mobileconnect://connect[/]?[name=*ConnectionName*|**server=***ServerAddress*]
[**&***Parameter1*=*Value*&*Parameter2*=*Value...*]

Following are examples of the mobileconnect command:

```
mobileconnect://connect/?name=Example
sonicwallmobileconnect://connect/?name=Example
mobileconnect://connect?name=Example
mobileconnect://connect?server=vpn.example.com
mobileconnect://connect?name=Example%202&server=vpn.example.com
mobileconnect://
connect?name=SRA%20Connection&server=sslvpn.example.com&username=test
&password=password&domain=LocalDomain
mobileconnect://connect?name=EX%20Connection&server=
workplace.example.com&username=test&password=password&realm=Corp
```

Connect Command Parameters

Command Parameter	Description
name	The unique name of the VPN connection entry that will be created and appear in the Mobile Connect Connections list. Mobile Connect accepts the name only if it is unique. Letters are case sensitive.
server	The domain name or IP address of the Dell SonicWall appliance in which you wish to connect. For example: vpn.example.com
username	**Optional**: The username used in the VPN connection.
password	**Optional**: The password used in the VPN connection.
realm	**Optional**: The realm used in the VPN connection profile. Applies to EX series connections only.
domain	**Optional**: The domain used in the VPN connection profile. Applies to SRA and UTM connections only.
sessionid	**Optional**: The session ID or Team ID used for authentication.
connect	**Optional**: If presented and the value is non-null, the connection will be initiated if the profile was successfully added.
callbackurl	**Optional**: The callback URL is be opened by Mobile Connect after the connect command has been processed. See Connect Command on page 19 for full details of the callback URL syntax and options.

Disconnect Command

The disconnect command is used to disconnect an active connection. In addition, a callback URL can be provided that Mobile Connect will open after the connection is disconnected, which makes it possible to return to the calling app. If there is no active VPN connection, the command is ignored.

Syntax:

```
mobileconnect://disconnect[/]
mobileconnect://disconnect[/]?[callbackurl=<callbackurl>]
```

Following are examples of the disconnect command:

```
mobileconnect://disconnect
```

```
mobileconnect://disconnect/
```

```
sonicwallmobileconnect://disconnect
```

```
mobileconnect://
disconnect?callbackurl=customapp%3A%2F%2Fhost%3Fstatus%3D%24STATUS%24%
26login_group%3D%24LOGIN_GROUP%26error_code%3D%24ERROR_CODE%24
```

```
sonicwallmobileconnect://
disconnect?callbackurl=customapp%3A%2F%2Fhost%3Fstatus%3D%24STATUS%24%
26login_group%3D%24LOGIN_GROUP%26error_code%3D%24ERROR_CODE%24
```

Disconnect Command Parameters

Command Parameter	Description
`callbackurl`	**Optional**: The callback URL is opened by Mobile Connect after the disconnect command has been processed. See Disconnect Command on page 20 for full details of the callback URL syntax and options.

Callback URL

While invoking Mobile Connect using a URL, a third party application can include a callback URL that is called by Mobile Connect once it completes the requested action. The callback URL value may also contain special tokens that will be evaluated and dynamically replaced by Mobile Connect to provide additional status and connection information back to the app that is opened by the callback URL. Tokens are evaluated in place, in the same order in which the tokens were specified.

To ensure that it functions properly, the base callback URL format should be RFC 1808 compliant and should be able to be launched independently of Mobile Connect. For example it should launch through a web page or iOS web clip.

```
URL: <scheme>://<net_loc>/<path>;<params>?<query>#<fragment>
```

Note The value of callbackurl must also be properly URL encoded to ensure that Mobile Connect can process the callback URL correctly.

Dynamic Tokens Supported by the Callback URL

Dynamic Token	Description
`$ERROR_MESSAGE$$`	The string value of the error message from the failed connection attempt.
`$LOGIN_GROUP$`	The string value of the authentication login group or realm. Applies to EX series connections only.
`$COMMUNITY$`	The string value of authentication community. Applies to EX series connections only.
`$ZONE$`	The string value of EPC zone. Applies to EX series connections only.
`$TUNNEL_IP$`	The string value of the Mobile Connect IPv4 client address.

Dynamic Token	Description
$TUNNEL_MODE$	One of split, split-nonlocal, redirectall, or redirectall-nonlocal depending on the tunnel mode. Applies to SRA and UTM connections only.
$ESP_ENABLED	Yes, or no depending on if ESP is enabled. Applies to SRA and UTM connections only.

Note Any number of tokens from the table above can be specified.

Following are examples using the callback URL:

Callback URL

```
customapp://host?status=$STATUS$&login_group=$LOGIN_GROUP&
error_code=$ERROR_CODE$
```

Full URL with URL Encoded Callback URL Value

```
mobileconnect://connect?sessionid=<teamid>&callbackurl=customapp%3A%2F%
2Fhost%3Fstatus%3D%24STATUS%24%26login_group%3D%24LOGIN_GROUP%
26error_code%3D%24ERROR_CODE%24
```

Callback URL

```
myapp://callback?status=$STATUS$&login_group=$LOGIN_GROUP&
error_code=$ERROR_CODE$
```

Full URL with URL Encoded Callback URL Value

```
mobileconnect://connect?sessionid=<teamid>&callbackurl= myapp%3A%2F%
2Fcallback%3Fstatus%3D%24STATUS%24%26login_group%3D%24LOGIN_GROUP%
26error_code%3D%24ERROR_CODE%24
```

Callback URL

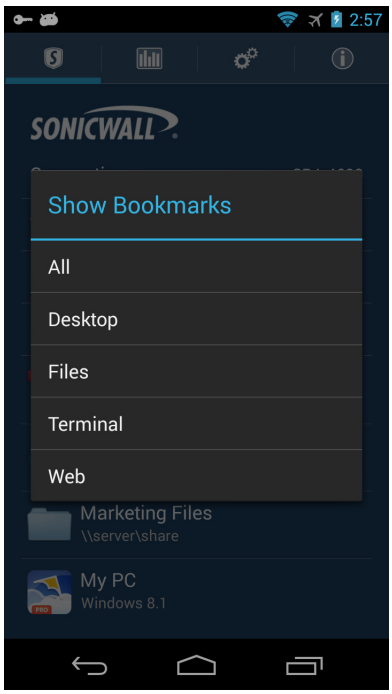
```
http://server/example%20file.html
```

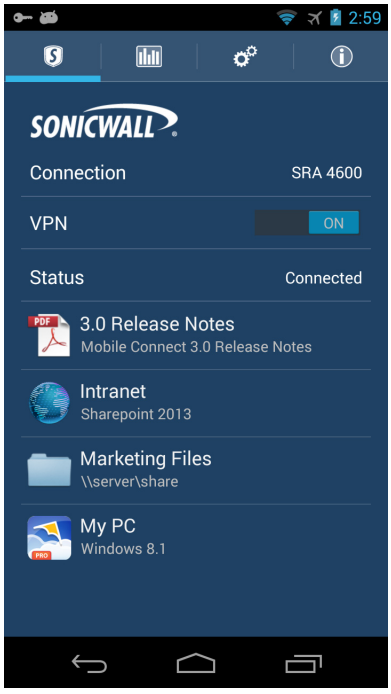
Full URL with URL Encoded Callback URL Value

```
mobileconnect://connect?callbackurl=http%3A%2F%2Fserver%2Fexample%2520file.html
```

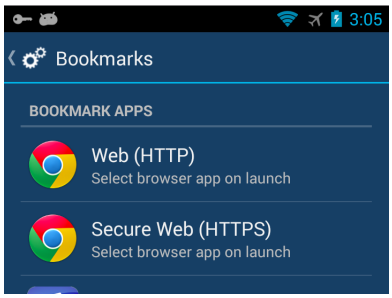
Bookmarks

When there are more than five bookmarks, the bookmarks are replaced by a Filter screen that groups bookmarks by type. Select the type of bookmarks to display or select **All Bookmarks** to display all bookmarks. Note that for the SRA appliances, the server must be running version 7.0 or higher.





Selecting a bookmark for an app that is not installed will prompt you to install the app. Apps referenced by bookmarks also can be installed at any time using the Settings > Bookmarks tab. In addition to installing apps for bookmarks, the Settings > Bookmarks tabs is also used to select and install apps for bookmarks that support multiple third party apps. For example, you might select Chrome or Firefox for a Web bookmark.



Mobile Connect supports the following types of bookmarks and associated apps.

Desktop Bookmarks:

Portal name: Terminal Services (RDP – ActiveX), Terminal Services (RDP – Java) Internal type: RDP5ActiveX, RDP5Java

RDP bookmark types attempt to launch with the associated RDP application, as configured in the Settings tab.

	Android Version
Wyse PocketCloud Pro	1.4.217
2X Client RDP/Remote Desktop	11.0.1899
Remote RDP Lite	4.2.8
Remote RDP	4.2.8
Remote RDP Enterprise	4.2.8
Microsoft Remote Desktop	8.0.5

Additional details such as screen resolution should be provided to the client. However, support for passing such parameters will vary based on the application. For example:

- Wyse PocketCloud Pro does not support the “connect to console” option

Portal name: Virtual Network Computing (VNC)
Internal type: VNC

VNC bookmark types attempt to launch with the associated VNC application as configured in the Settings tab.

	Android Version
Wyse PocketCloud Pro	1.4.217
android-vnc-viewer	0.5.0

Additional details such as screen resolution should be provided to the client. However, support for passing such parameters varies based on the application.

Portal name: Citrix Portal (Citrix)
Internal type: Citrix, Citrix_https

Citrix bookmark types will attempt to launch with the associated Citrix application.

	Android Version
Citrix Receiver	3.4.13

Additional details such as screen resolution should be provided to the client. However, support for passing such parameters will very based on the application.

Web Bookmarks:

Portal name: Web (HTTP), Secure Web (HTTPS), External Web Site
Internal type: HTTP, HTTPS, URL, URL_https

These bookmarks will launch in an associated web browser and the provided 'Name or IP Address' (HostID) will be passed as the parameter to display in the browser.

	Android Version
Any Browser	Yes
Google Chrome	33.0.1750.170

Portal name: Mobile Connect
Internal type: MC

Mobile Connect bookmark type will rely fully on the OS to determine and launch the proper application. The bookmark is expected to be properly configured for launch. The Mobile Connect app will attempt to launch it as is. (for example, telnet://server)

Terminal Bookmarks:

Portal name: Telnet, Secure Shell Version 1 (SSHv1), Secure Shell Version 2 (SSHv2)
Internal type: Telnet, SSH, SSHv1

	Android Version
ConnectBot	1.7.1

ConnectBot notes: Proper formatting is required for ConnectBot SSH (server bookmark field requires username@server).

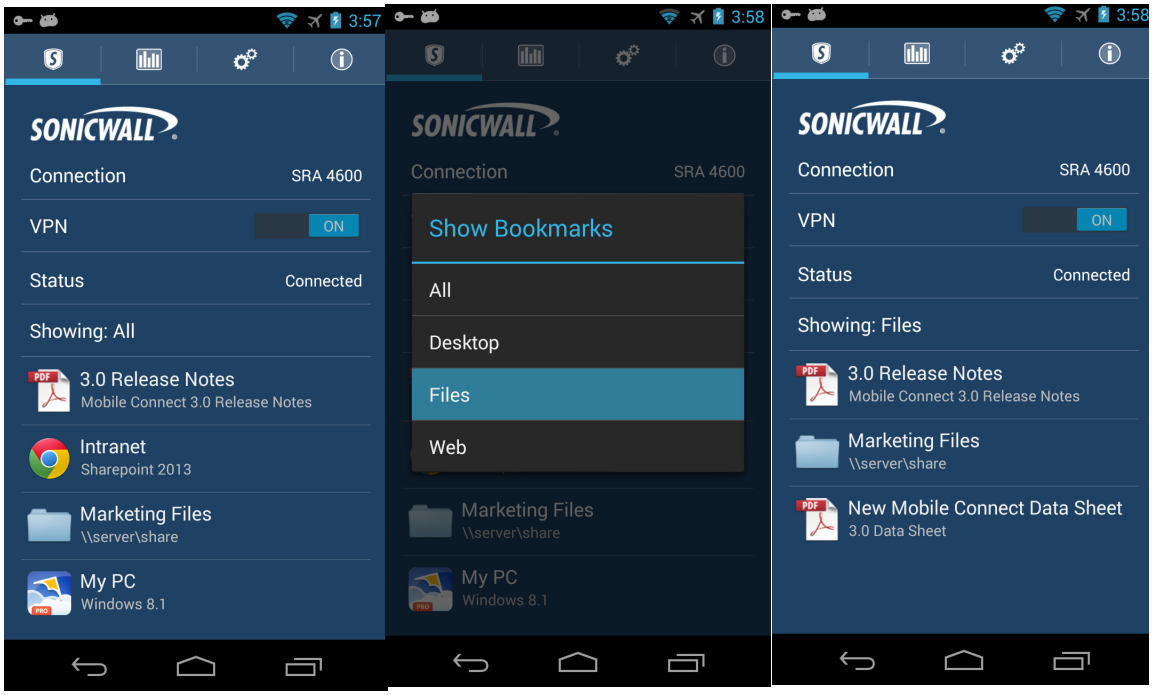
Note Some supported third party apps may not yet be available in the Amazon Appstore.

Files

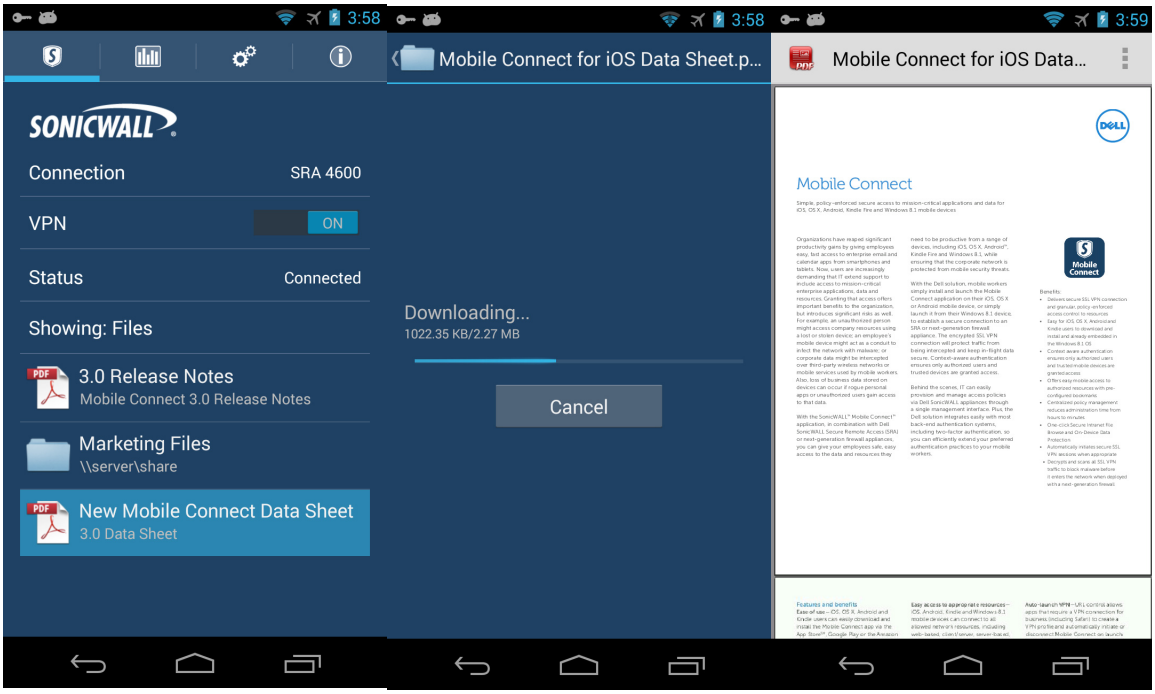
Mobile Connect 3.0 introduces secure mobile access to files through new File bookmarks. File bookmarks are displayed after the VPN is connected in the table of bookmarks. Tapping a File bookmark allows secure access to files by first checking and enforcing the server configured file policy, and then securely downloading and displaying the file within the Mobile Connect app, On Android, policies include control over whether a file may be opened in a third-party app or securely cached on the device. File bookmarks can also be created to folders or file share root directories to allow directory navigation.

Note Note In Mobile Connect for Android 3.0, Files bookmarks are supported on the Dell SonicWALL SRA appliances starting with SRA 7.5 firmware. Support for Files in E-Series SRA and NGFW is expected in a future release.

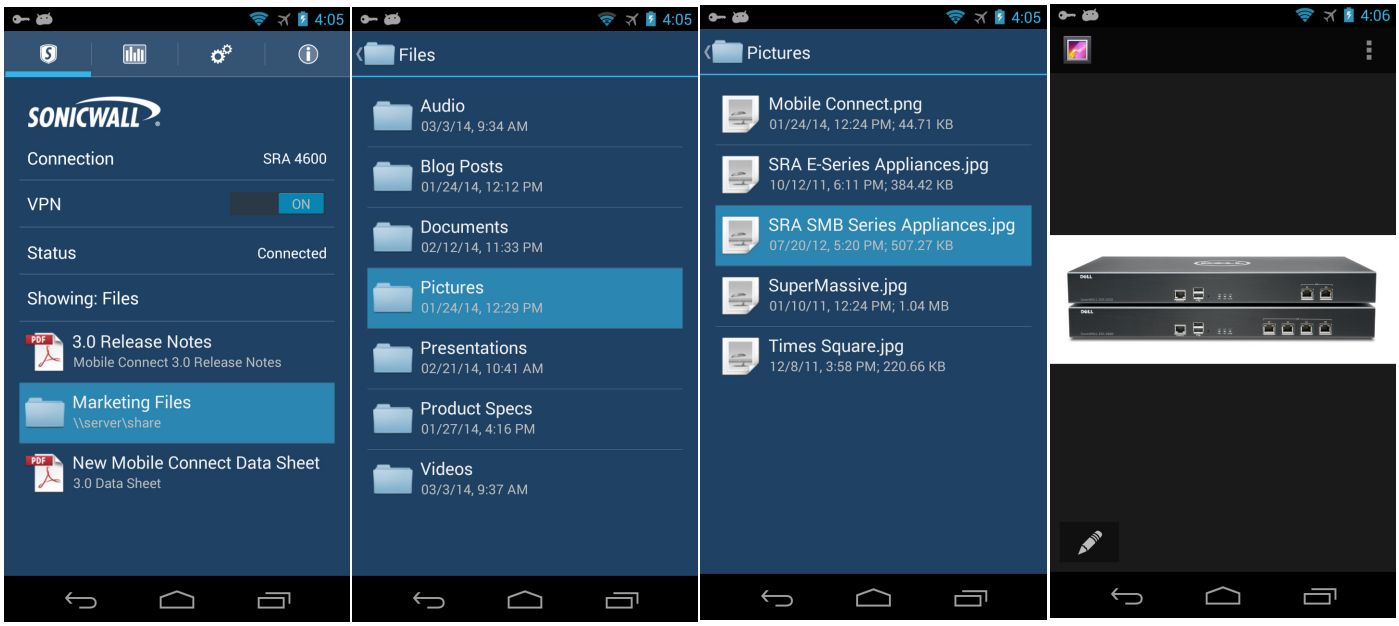
When Files bookmarks are configured for the user on the server appliance, they appear in the list of bookmarks after the VPN is established and can be filtered by selecting the **Showing: Files** row that is displayed when there are more than five bookmarks.



Tapping a File bookmark queries and enforces the server-configured file policy for that file bookmark. If the file is not already cached on the device, it securely downloads the file from the SRA appliance. Once the file is downloaded, it is opened in the Android default file viewer app for that file type.



Tapping a File bookmark to a folder or directory allows for directory browsing and file download and viewing of any file in the folder. All attempts to browse a file folder or view a file query the server to enforce access policies. On Android, the default file viewer app is automatically launched after a file is downloaded.



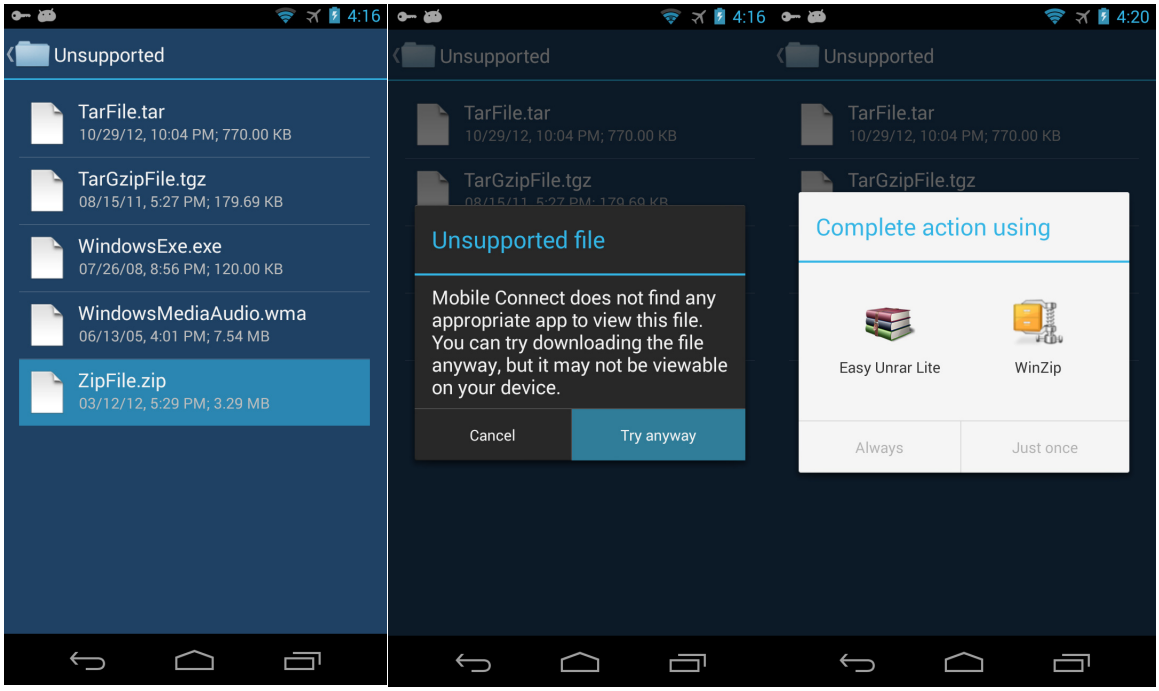
Supported File Types

Mobile Connect supports all file types natively supported by Android, including the following:

	File Extension
Images	.jpg, .jpeg, .tif, .tiff, .png
Music	.mp3, .m4a, .wav
Movies	.mov, .mp4
Microsoft Word Documents	.doc, .docx
Microsoft Excel Spreadsheets	.xls, .xlsx
Microsoft Powerpoint Presentations	.ppt, .pptx
Adobe PDF	.pdf
Web Pages	.htm, .html
Text and Rich-text Files	.txt, .rtf

Unsupported Files

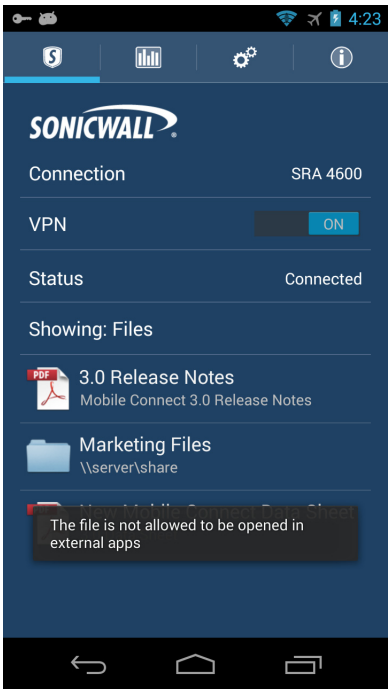
If a file type is not supported, the user will be prompted that the file may not be viewable unless there is another app installed that can view the file. The user can tap ‘Try Anyway’ and if there is another app that is registered to handle that file type, the user will have the option to open the file in that app.



File Policies

On Android, server-configured policies control whether a file can be opened in a third-party app or securely cached on the device.

For example, if a file has the *Allow Open In* policy disabled, the file cannot be viewed on an Android device. Mobile Connect launches third-party apps to view all file types, so the *Allow Open in* policy must be enabled to view a file.

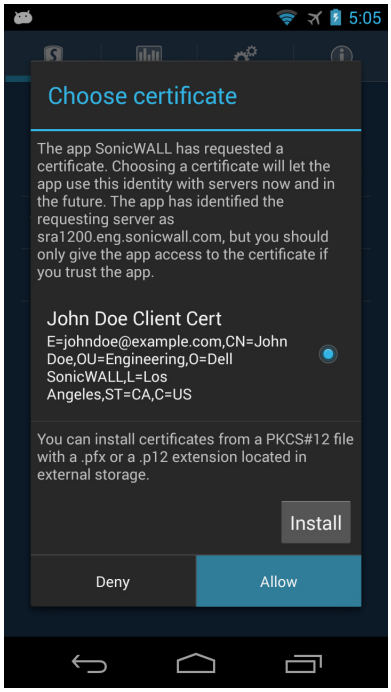


Configure Client Certificates

Note Client certificate support is only available for connections to Dell SonicWALL E-Class SRA and SMB SRA appliances.

Configuring a Connection to Dell SonicWALL E-Class SRA Appliances

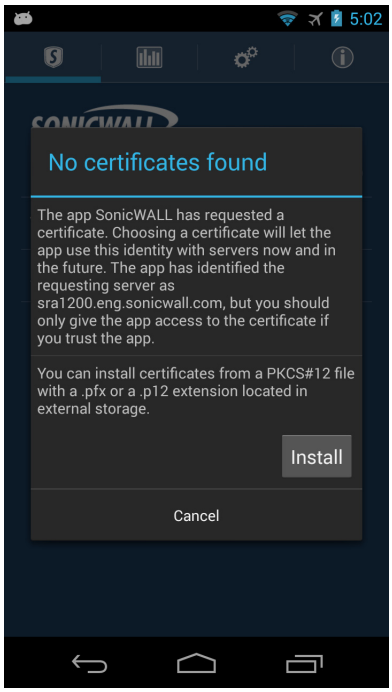
If a client certificate is required during authentication, you are automatically prompted to select a client certificate from the Android device client certificate store.


5:05
Choose certificate
The app SonicWALL has requested a certificate. Choosing a certificate will let the app use this identity with servers now and in the future. The app has identified the requesting server as sra1200.eng.sonicwall.com, but you should only give the app access to the certificate if you trust the app.
John Doe Client Cert
E=johndoe@example.com,CN=John Doe,OU=Engineering,O=Dell SonicWALL,L=Los Angeles,ST=CA,C=US
You can install certificates from a PKCS#12 file with a .pfx or a .p12 extension located in external storage.
Install
Deny
Allow

Select the client certificate from the list of certificates and tap **Allow**.

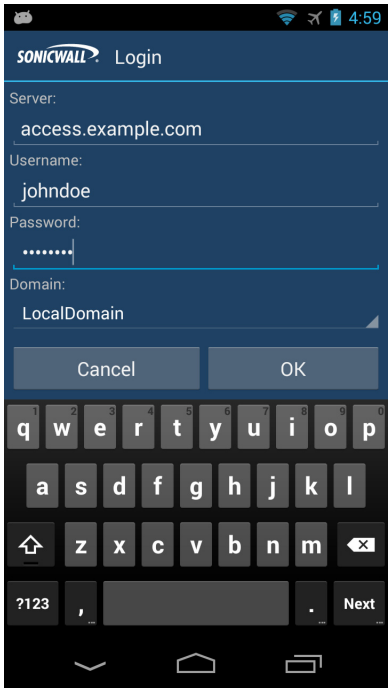
By default a VPN configuration prompts you to select the client certificate during authentication. If you successfully authenticate with a client certificate, the VPN configuration profile is automatically updated to use the client certificate for each subsequent connection attempt. To reset the client certificate selection, edit the connection and tap the **Forget Selections** button.

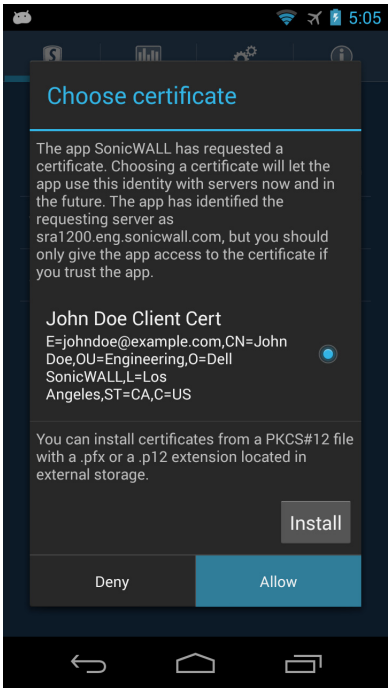
Note If no client certificates are installed, an Android *No certificates found* dialog appears with an option to install a PKCS#12 file located in external storage.


5:02
No certificates found
The app SonicWALL has requested a certificate. Choosing a certificate will let the app use this identity with servers now and in the future. The app has identified the requesting server as sra1200.eng.sonicwall.com, but you should only give the app access to the certificate if you trust the app.
You can install certificates from a PKCS#12 file with a .pfx or a .p12 extension located in external storage.
Install
Cancel

Configuring a Connection to Dell SonicWALL SMB SRA Appliances

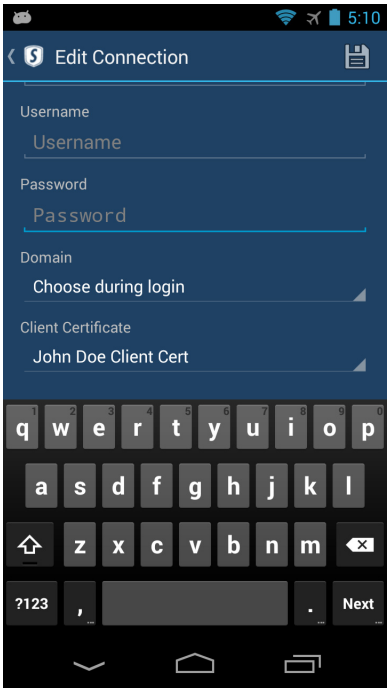
On SMB SRA appliances, client certificate authentication is available as a second factor authentication method in addition to standard user name and password authentication. If a client certificate is required during authentication, you are automatically prompted to select a client certificate from the Android device client certificate store.




5:05
Choose certificate
The app SonicWALL has requested a certificate. Choosing a certificate will let the app use this identity with servers now and in the future. The app has identified the requesting server as sra1200.eng.sonicwall.com, but you should only give the app access to the certificate if you trust the app.
John Doe Client Cert
E=johndoe@example.com,CN=John Doe,OU=Engineering,O=Dell SonicWALL,L=Los Angeles,ST=CA,C=US
You can install certificates from a PKCS#12 file with a .pfx or a .p12 extension located in external storage.
Install
Deny
Allow

Select the client certificate from the list of certificates and tap **Allow**.

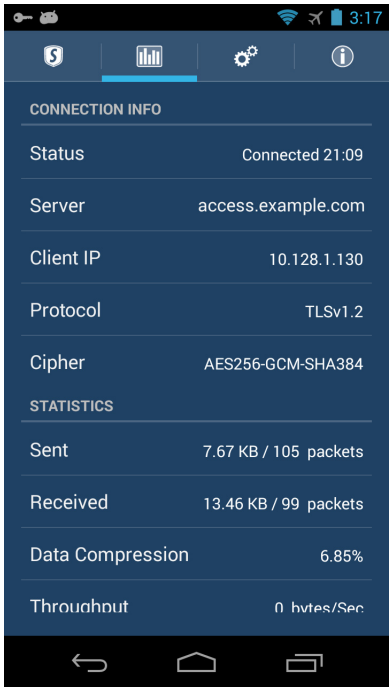
By default the client certificate is set to **Choose during login** for a VPN configuration. If you successfully authenticate with a client certificate, the VPN configuration profile is automatically updated to set the client certificate to the one that was chosen. To reset the client certificate selection, edit the connection and set the Client Certificate field back to **Choose during login**.



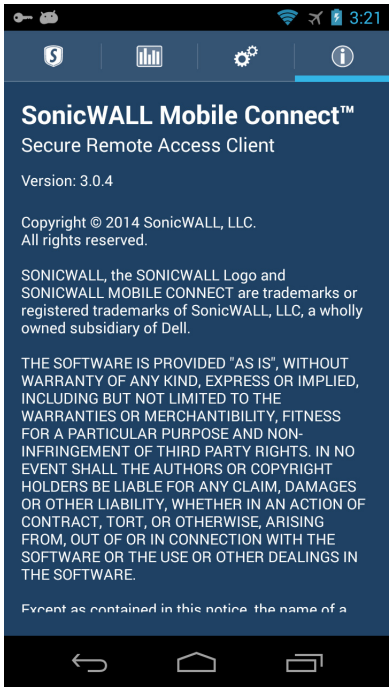
Note If no client certificates are installed, an Android *No certificates found* dialog appears with an option to install a PKCS#12 file located in external storage.

Monitoring Mobile Connect

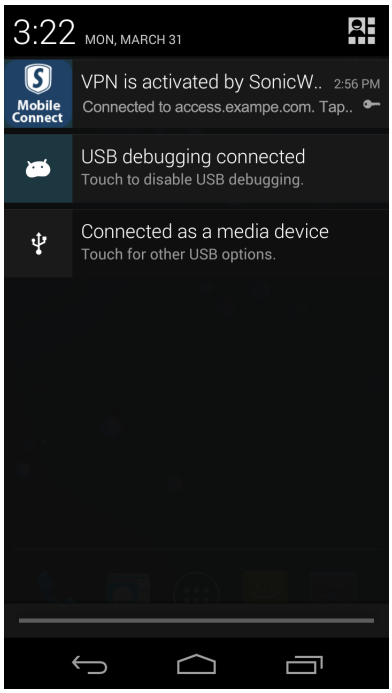
The **Monitor** tab displays additional details about the connection, statistics on traffic transmitted, DNS information, and routes that have been installed.



The **About** tab of SonicWALL Mobile Connect displays the version number and legal text.

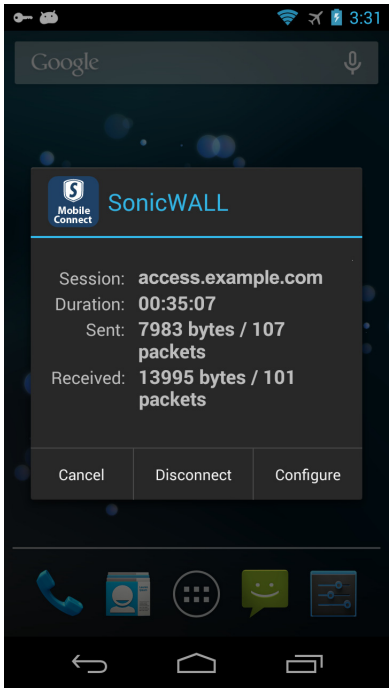

3:21
SonicWALL Mobile Connect™
Secure Remote Access Client
Version: 3.0.4
Copyright © 2014 SonicWALL, LLC.
All rights reserved.
SONICWALL, the SONICWALL Logo and SONICWALL MOBILE CONNECT are trademarks or registered trademarks of SonicWALL, LLC, a wholly owned subsidiary of Dell.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OR MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT, OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

When a Mobile Connect session is active, the Android System Notifications area includes an entry indicating that the VPN is connected.



Tapping on the SonicWALL Mobile Connect entry in the Android System Notifications area displays a summary of statistics on the VPN session. The statistics page displays the server name, duration of the session, and the amount of traffic that has been sent and received. Three buttons are also provided on this screen:

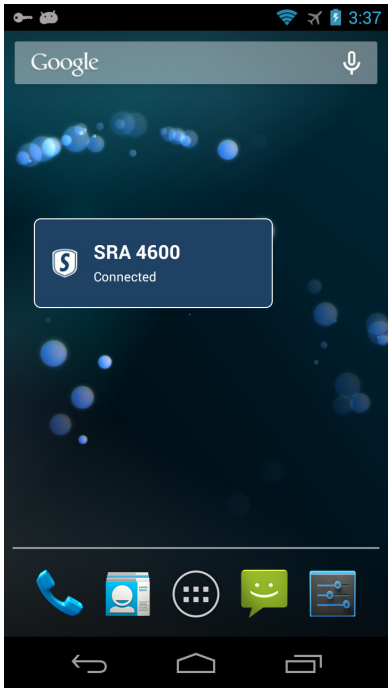
- **Cancel** – Closes the statistics screen.
- **Disconnect** – Disconnects the Mobile Connect session.
- **Configure** – Launches the SonicWALL Mobile Connect app.



Mobile Connect Widget

When the SonicWALL Mobile Connect app is installed, a widget for Android is also created in the widgets tab. It can then be dragged from the widgets tab to the home screen. This widget is used as follows:

- The widget shows the connection status (connected, disconnected, connecting, etc.)
- Tap the icon to establish a tunnel when disconnected.
- Tap the icon to disconnect the tunnel when connected.
- Tap any other area of the widget to launch the Mobile Connect client.



Troubleshooting Mobile Connect

If you are unable to connect to the Dell SonicWALL server, perform the following steps to troubleshoot the connection.

1. Double check that you have entered the server name properly in the connection configuration.
2. Go to the web browser on your device and attempt to navigate to the SSL VPN appliance web portal.
3. If you are unable to load the web portal, the problem is with the Dell SonicWALL appliance. Contact your network administrator if the problem persists.
4. If the web portal loads successfully on the browser and you still cannot establish a Mobile Connect connection, notify Dell SonicWALL Support, as follows:
   a. On the **Settings** tab, enable the **Debug Logging** option.
   b. Attempt a connection to the server again to ensure that full debugging messages are logged for the attempt.
   c. Then return to the **Settings** tab and tap the **Email Logs** button. An email will launch in your mail client with the Mobile Connect log attached. Address the email to **Support@sonicwall.com**. Add any additional comments to the email and tap **Send**. Dell SonicWALL Support staff will contact you after reviewing your case.